involve
a journal of mathematics

Conjugation diameter of the symmetric groups

Assaf Libman and Charlotte Tarry

msp

2020 vol. 13, no. 4

INVOLVE 13:4 (2020)
https://doi.org/10.2140/involve.2020.13.655

Conjugation diameter of the symmetric groups

Assaf Libman and Charlotte Tarry

(Communicated by Kenneth S. Berenhaut)

The conjugation diameter of a group G is the largest diameter of its Cayley graphs with respect to conjugation-invariant generating sets. It is a strong form of the extensively studied concept of the diameter of G. We compute the conjugation diameter of the symmetric groups.

1. Introduction and main results

Let G be a finite group. Let $\operatorname{diam}(G, S)$ denote the diameter of the associated Cayley graph $\Gamma(G, S)$ with respect to a generating set S. Set $\operatorname{diam}(G) = \sup\{\operatorname{diam} \Gamma(G, S)\}$, where the supremum is taken over all generating sets S. This concept has been studied for several decades and was the subject of intensive activity; see [Babai et al. 1990], which gives a good survey. Particular attention was given to the diameter of the symmetric groups [Babai and Seress 1992; Helfgott and Seress 2014] due to its relevance in computing science and networks [Preparata and Vuillemin 1981].

In this note we study the *conjugation diameter* of a group G, which we denote by $\Delta(G)$. That is, $\Delta(G) = \sup\{\operatorname{diam} \Gamma(G, S)\}$, where S runs through all generating sets which are *conjugation-invariant and conjugation-finite*, i.e., unions of finitely many conjugacy classes in G. Conjugation diameter has been studied under the name C-width by Bardakov, Tolstykh and Vershinin [Bardakov et al. 2012].

Kędra, Martin and the first author had a geometric motivation in studying conjugation diameter. Any generating set S gives rise to a word norm on G, namely the minimum length of a word in $S \cup S^{-1}$ needed to express an element of G. Then $\operatorname{diam}(G, S)$ is the diameter of G with respect to this norm and is a measure of the "efficiency" S generates. If S is conjugation-invariant then so is the associated word norm. Conjugation-invariant norms were studied by Burago, Ivanov and Polterovich [Burago et al. 2008], who introduced the concept of bounded groups, namely groups for which every conjugation-invariant norm has finite diameter. In [Kędra et al. 2018] Kędra, Martin and the first author gave several refinements of this concept for groups G which are finitely normally generated; namely there exists a finite

MSC2010: 05E15, 20B30.
Keywords: conjugation diameter, symmetric groups.

$X \subseteq G$ such that $\langle\langle X \rangle\rangle = G$. These refinements are defined by the diameter of G with respect to conjugation-invariant word norm and are therefore related to $\Delta(G)$.

For example, it is shown in [Kędra et al. 2018, Theorem 6.3] that all noncompact connected semisimple Lie groups G are uniformly bounded, namely $\Delta(G) < \infty$. In fact (unpublished notes) it can be shown that $\Delta(\mathrm{SL}(2, \mathbb{R})) = 4$ and $\Delta(\mathrm{PSL}(2, \mathbb{R})) = 3$ and $\Delta(\mathrm{SL}(2, \mathbb{C})) = 3$ and $\Delta(\mathrm{PSL}(2, \mathbb{C})) = 2$. The second author showed in [Tarry 2020, Chapter 7] that $\Delta(\mathrm{PSL}(n, \mathbb{C})) \leq 6(n-1)$ for all $n \geq 3$. If R is a principal ideal domain with only $d < \infty$ maximal ideals then $\Delta(\mathrm{PSL}(n, R)) \leq 12d(n-1)$ for any $n \geq 3$ [Kędra et al. 2018, Theorem 6.3].

In general, calculating $\Delta(G)$ is difficult and the purpose of this note is to compute this invariant for some finite groups. If G is finite abelian then $\Delta(G) = \mathrm{diam}(G)$, which was calculated in [Klopsch and Lev 2003], where they showed that if $G = C_{n_1} \times \cdots \times C_{n_r}$ is the canonical decomposition [Rotman 1973, Corollary 4.7], where $n_1 \mid \cdots \mid n_r$, then $\Delta(G) = \sum_i \lfloor n_i/2 \rfloor$. Here $\lfloor x \rfloor$ is the floor of x.

Beyond abelian groups calculations are more involved. Let $p < q$ be distinct primes such that $p \mid (q-1)$ and let G be the unique nonabelian group of order pq. An easy application of Sylow's theorems gives the following theorem, which should be compared with [Babai and Seress 1992, Proposition 5.5], where it is shown that $\mathrm{diam}(G) < 3q$.

Theorem 1.1. *Let $p < q$ be primes and G a nonabelian group of order pq. Then*

$$\Delta(G) = \max\left\{\tfrac{p-1}{2}, 2\right\}.$$

The main result of this paper is the calculation of the conjugation diameter of the symmetric groups. It should be compared with the celebrated results in [Helfgott and Seress 2014].

Theorem 1.2. *Let S_n denote the symmetric group, $n \geq 2$. Then*

$$\Delta(S_n) = n - 1.$$

2. Norms and conjugation diameter

Let X be a subset of a group G. Set $X^{-1} = \{x^{-1} : x \in X\}$. If $X, Y \subseteq G$ set $XY = \{xy : x \in X, y \in Y\}$ and let X^n denote $X \cdots X \subseteq G$ (n factors).

Definition 2.1. Let X be a subset of a group G. Set $\mathrm{ccs}(X) = \{gxg^{-1} : x \in X, g \in G\}$, the union of the conjugacy classes of the elements of X. For any $n \geq 0$ define subsets $B_X(n)$ of G as follows. Set

$$B_X(0) = \{1\} \quad \text{and} \quad B_X(1) = \{1\} \cup \mathrm{ccs}(X) \cup \mathrm{ccs}(X^{-1}).$$

For any $n \geq 1$ set

$$B_X(n) = B_X(1)^n \subseteq G.$$

If $X = \{g\}$ is a singleton, we will often write $B_g(n)$.

Thus, $B_X(n)$ is the set of all "words" of length at most n in the conjugates of the elements of X and their inverses. The following proposition follows directly from the definitions. See [Kędra et al. 2018, Lemma 2.3] and [Tarry 2020, Lemma 1.15] for details.

Proposition 2.2. *Let X, Y be subsets of G:*

(i) *$B_X(n)$ is closed under conjugation in G.*

(ii) *If $X \subseteq Y$ then $B_X(n) \subseteq B_Y(n)$ for all $n \geq 0$.*

(iii) *$B_X(m) \cdot B_X(n) = B_X(m+n)$.*

(iv) *If $Y \subseteq B_X(n)$ for some $n \geq 0$ then $B_Y(m) \subseteq B_X(mn)$ for all $m \geq 0$.*

Definition 2.3. We say that $X \subseteq G$ *normally generates* G if $G = \langle\langle X \rangle\rangle$. We say that G is *finitely normally generated* if it contains a finite normally generating set.

Note that X normally generates G if and only if $\bigcup_{n \geq 0} B_X(n) = G$. Thus, the following definition makes sense (the minimum is taken over a nonempty set of integers).

Definition 2.4. Suppose that X normally generates G. Define $\|\cdot\|_X : G \to \mathbb{R}$ by

$$\|g\|_X = \min\{n \geq 0 : g \in B_X(n)\}.$$

Clearly $\|\cdot\|_X$ is a conjugation-invariant norm on G [Tarry 2020, Proposition 1.19]. We define

$$\|G\|_X = \operatorname{diam}(G, \|\cdot\|_X) = \sup\{\|g\|_X : g \in G\}.$$

It is immediate from the definitions that

$$\|G\|_X = \inf\{n : G \subseteq B_X(n)\}. \tag{1}$$

In particular if $X \subseteq Y$ normally generate G then $\|G\|_Y \leq \|G\|_X$. Clearly, $B_X(n)$ is the closed ball of radius n centred at $1 \in G$ with respect to the metric $\|\cdot\|_X$ induces on G.

Definition 2.5. The *conjugation diameter* of a finitely normally generated group G is

$$\Delta(G) = \sup\{\|G\|_X : X \subseteq G \text{ normally generates } G \text{ and } |X| < \infty\}.$$

We call G *uniformly bounded* if $\Delta(G) < \infty$; see [Kędra et al. 2018, Definition 2.6].

3. pq-groups

Proof of Theorem 1.1. Let Q be a Sylow q-subgroups of G. Then $Q \trianglelefteq G$ since $p < q$. Since G is not abelian, no Sylow p-subgroup of G can be normal and no element of G has order pq.

Our first goal is to prove that any $g \in G$ of order p normally generates G and

$$\|G\|_g = \max\left\{2, \tfrac{p-1}{2}\right\}. \tag{2}$$

Let $C_G(g)$ be the centraliser of g. Then either $|C_G(g)| = p$ or $|C_G(g)| = pq$ since $g \in C_G(g)$. The latter is impossible since it implies that $\langle g \rangle$ is a central Sylow p-subgroup of G. We deduce that $|C_G(g)| = p$ and therefore

$$|\mathrm{ccs}(g)| = [G : C_G(g)] = q.$$

Consider the quotient homomorphism $\pi : G \to G/Q$. Since $G/Q \cong C_p$ is abelian, π must be constant on conjugacy classes of G. Then $\mathrm{ccs}(g) \subseteq gQ$ since $\pi(\mathrm{ccs}(g)) = \bar{g}$ and equality holds since they have the same cardinality.

By Definition 2.1, and since $Q \trianglelefteq G$,

$$B_g(1) = \{1\} \cup gQ \cup g^{-1}Q.$$

Since $Q \not\subseteq B_g(1)$, it follows that $\|G\|_g > 1$. Also, $gQ \cdot g^{-1}Q = Q$, which implies that $B_g(2) = g^{-2}Q \cup g^{-1}Q \cup Q \cup gQ \cup g^2Q$. Using induction one shows that

$$B_g(n) = \bigcup_{k=-n}^{n} g^k Q, \quad n \geq 2.$$

Now, $\langle g \rangle$ is a Sylow p-subgroup of G and its elements form a complete set of representatives for the cosets of Q. If $p = 2$ or $p = 3$ then $\langle g \rangle = \{1, g^{\pm 1}\}$ and therefore $B_g(2) = G$ so $\|G\|_g = 2$. If $p > 3$ then p is odd and $\frac{p-1}{2} \geq 2$ and

$$\langle g \rangle = \left\{g^k : -\tfrac{p-1}{2} \leq k \leq \tfrac{p-1}{2}\right\}.$$

Therefore $B_g\left(\frac{p-1}{2}\right) = G$ and $B_g(n) \neq G$ if $n < \frac{p-1}{2}$. It follows that $\|G\|_g = \frac{p-1}{2}$ in this case and we have established (2). In particular

$$\Delta(G) \geq \max\left\{\tfrac{p-1}{2}, 2\right\}.$$

Let $X \subseteq G$ be any normally generating subset of G. No element of order pq exists and if all elements of X have order q then $\langle\langle X \rangle\rangle = Q \trianglelefteq G$, a contradiction. So there exists $g \in X$ of order p and we have seen that g normally generates G and

$$\|G\|_X \leq \|G\|_g = \max\left\{\tfrac{p-1}{2}, 2\right\}.$$

It follows that $\Delta(G) \leq \max\left\{\frac{p-1}{2}, 2\right\}$ and equality holds. □

4. The symmetric groups

4.1. *Notation and basic facts.* Conjugation of elements $g, h \in G$ is denoted by

$$g^h = hgh^{-1}.$$

Any $\sigma \in S_n$ can be written as a product of disjoint cycles of lengths $k_1, \ldots, k_r$, where $k_i \geq 1$ and $\sum_i k_i \leq n$. We call σ a $(k_1, \ldots, k_n)$-*cycle*. Cycle structure determines the conjugacy class [Hall 1959, Theorem 5.13] and we denote the conjugacy class of σ by

$$[k_1, \ldots, k_m].$$

Conjugation of a k-cycle $(i_1 \cdots i_k)$ by $\tau \in S_n$ is the k-cycle $(\tau(i_1) \cdots \tau(i_k))$ [Rotman 1973, Lemma 3.9]. The inverse of a k-cycle is a k-cycle and hence any $\sigma \in S_n$ is conjugate to σ^{-1}.

Let $\mathrm{fix}(\sigma)$ denote the set of fixed points and $\mathrm{supp}(\sigma)$ denote the support. If $\mathrm{fix}(\sigma)$ is not empty then σ is conjugate to $\sigma' \in S_{n-1}$.

Lemma 4.2. *Consider $\tau \in S_n$. Then $B_\tau(n)$ is the set of elements of the form $\tau^{\lambda_1} \cdots \tau^{\lambda_\ell}$, with conjugation by $\lambda_1, \ldots, \lambda_\ell \in S_n$, where $\ell \leq n$.*

Proof. The elements of $B_\tau(n)$ are products of at most n conjugates of $\tau^{\pm 1}$. Since τ^{-1} is conjugate to τ the result follows. □

Lemma 4.3. *Suppose that $\tau \in S_n$ is a product $\tau = \alpha\beta$ of permutations with disjoint supports, where $\alpha \in S_k$ and $\beta \in S_{n-k}$ for some k. Then $B_\tau(2)$ contains all elements of the form $\alpha^{\lambda_1}\alpha^{\lambda_2}$ for any $\lambda_1, \lambda_2 \in S_k$.*

Proof. Choose $\theta \in S_{n-k}$ such that $\beta^\theta = \beta^{-1}$. Then $\tau^{\lambda_1}\tau^{\lambda_2\theta} = \alpha^{\lambda_1}\alpha^{\lambda_2}\beta\beta^\theta = \alpha^{\lambda_1}\alpha^{\lambda_2}$. □

Lemma 4.4. *Let $n \geq 2$:*

(i) *If $X \subseteq S_n$ normally generates S_n then X contains an odd permutation.*

(ii) *Conversely, any odd permutation normally generates S_n.*

Proof. (i) If X contains only even permutations then $\langle\langle X \rangle\rangle \subseteq A_n \trianglelefteq Sn$.

(ii) The only proper normal subgroups of S_n are A_n and the Klein group $K \subseteq A_4$ if $n = 4$. □

Obtaining a lower bound for $\Delta(S_n)$ is easy.

Proposition 4.5. *Let $\tau \in S_n$ be a transposition. Then τ normally generates S_n and $\|S_n\|_\tau = n - 1$.*

Proof. Any permutation is a product of 2-cycles, so τ normally generates. Any k-cycle is a product of $k-1$ transpositions; see [Rotman 1973, Proof of Theorem 3.4]. Hence any $\sigma \in [k_1, \ldots, k_m]$ is a product of $\sum_i k_i - m \leq n - m \leq n - 1$ transpositions. A product of m transpositions has at least $n - m$ orbits showing that an n-cycle cannot be written as a product of less than $n - 1$ transpositions. This shows that $\|S_n\|_\tau = n - 1$. □

Corollary 4.6. *We have $\Delta(S_n) \geq n - 1$ for any $n \geq 2$.*

Our goal now is to compute $\Delta(S_n)$. A major role will be played by 3-cycles and (2, 2)-cycles. An important feature they have is that we can obtain them "cheaply" from any nonidentity permutation.

Lemma 4.7. *Let $\tau \in S_n$ be a nonidentity element where $n \geq 4$. Then*:

(i) *$B_\tau(2)$ contains a 3-cycle if either τ is a transposition or if τ contains a cycle of length ≥ 3.*

(ii) *$B_\tau(2)$ contains a (2, 2)-cycle if τ is a transposition or it contains a (2, 2)-cycle or it contains a cycle of length ≥ 4.*

Proof. If τ is a transposition then $(1\,2)(2\,3) = (1\,2\,3)$ and $(1\,2)(3\,4)$ give the result. In the other cases, the calculations

$$(1\,2)(3\,4)\cdot(1\,3)(2\,4) = (1\,4)(2\,3),$$

$$(1\,2\,3\cdots k)\cdot(k\,k-1\cdots 3\,1\,2) = (1\,3\,2), \qquad k \geq 3,$$

$$(1\,2\,3\,4\cdots k)\cdot(k\,k-1\cdots 4\,1\,2\,3) = (1\,3)(2\,4), \quad k \geq 4,$$

together with Lemma 4.3, give the result. □

4.8. The next two propositions tell us that, with some fine print, by multiplying a 3-cycle τ with a permutation σ we may either

(a) split one of the cycles of σ into three disjoint parts, or

(b) fuse two disjoint cycles in σ and split the result in two, or

(c) fuse three cycles of σ into one cycle.

Clearly operations (a) and (c) are inverse of each other and the operation (b) is inverse to itself. Similarly, subject to some fine print, by multiplying a (2, 2)-cycle τ with σ we may either

(a) split one of the cycles of σ into three disjoint cycles, or

(b1) split two cycles of σ into two cycles each or,

(b2) fuse two cycles of σ and split the result into two cycles, or

(c1) fuse three cycles of σ, or

(c2) fuse two cycles and split a third, or

(d) fuse two pairs of disjoint cycles.

Thus, 3-cycles and (2, 2)-cycles provide us with a variety of "operations" on conjugacy classes in S_n.

The following calculations are left for the reader:

$$(1\,2\cdots m)\cdot(i\;j) = (1\cdots i\;j+1\cdots m)(i+1\cdots j), \quad 1 \leq i < j \leq m, \tag{3}$$

$$(1\,2\cdots \ell)(\ell+1\cdots m)\cdot(\ell\,m) = (1\,2\cdots m), \qquad 1 \leq \ell < m. \tag{4}$$

Proposition 4.9. *Let $C = [k_1, \dots, k_r]$ be a conjugacy class in S_n, where $k_i \geq 1$ and $\sum_i k_i \leq n$. Then $C \cdot [3]$ contains the following conjugacy classes in S_n, where $p', p'', p''' \geq 1$:*

(a) $[p', p'', p''', k_2, \dots, k_r]$, *where* $p' + p'' + p''' = k_1 \geq 3$.

(b) $[p', p'', k_3, \dots, k_r]$, *where* $r \geq 2$, $k_1 \geq 2$, $p' + p'' = k_1 + k_2$ *and* $p' \neq k_1$.

(c) $[k_1 + k_2 + k_3, k_4, \dots, k_r]$, *where* $r \geq 3$.

Proof. (a) Set $p = k_1$. Consider $1 < j < i \leq p$ (notice that $p \geq 3$). By inspection

$$(1\,2 \cdots p) \cdot (1\; i\; j) = (1\; i+1 \cdots p)(2 \cdots j)(j+1 \cdots i).$$

If $p' + p' + p''' = k_1$, set $j = p' + 1$ and $i = p' + p'' + 1$, and check that the resulting permutation belongs to $[p''', p'', p']$.

(b) Set $p = k_1$ and $q = k_2$. For any $i \neq p, p{+}q$ we have

$$(i\; p\; p{+}q) = (p\; p{+}q)(i\; p{+}q),$$

so (4) and (3) imply

$$(1\,2 \cdots p)(p+1 \cdots p{+}q) \cdot (i\; p\; p{+}q) = (1\,2 \cdots i)(i+1 \cdots p{+}q)$$

is a product of cycles of length i and $p + q - i$.

(c) Set $p = k_1$ and $q = k_2$ and $t = k_3$. By inspection

$$(1 \cdots p)(p+1 \cdots p{+}q)(p{+}q{+}1 \cdots p{+}q{+}t) \cdot (p\; p{+}q\; p{+}q{+}t) = (1\,2 \cdots p{+}q{+}t). \quad \square$$

Proposition 4.10. *Let $C = [k_1, \dots, k_r]$ be a conjugacy class in S_n, where $k_i \geq 1$ and $\sum_i k_i \leq n$. Then $C \cdot [2, 2]$ contains the following conjugacy classes in S_n, where $p', p'', p''', q', q'' \geq 1$:*

(a) $[p', p'', p''', k_2, \dots, k_r]$, *where* $p''' \geq 2$ *and* $p' + p'' + p''' = k_1 \geq 4$.

(b1) $[p', p'', q', q'', k_3, \dots, k_r]$, *where* $r \geq 2$ *and* $p' + p'' = k_1 \geq 2$.

(b2) $[p', p'', k_3, \dots, k_r]$, *where* $r \geq 2$, $p' + p'' = k_1 + k_2 \geq 4$, $p' \leq k_1 - 2$, *and if* $k_1 \geq 3$ *and* $k_2 \geq 2$ *then* $p' \leq k_1 - 1$.

(c1) $[k_1 + k_2 + k_3, k_4, \dots, k_r]$, *where* $r \geq 3$ *and* $k_1 \geq 2$.

(c2) $[p' + p'', k_2 + k_3, k_4, \dots, k_r]$, *where* $r \geq 3$ *and* $p' + p'' = k_1 \geq 2$.

(d) $[k_1 + k_2, k_3 + k_4, k_5, \dots, k_r]$, *where* $r \geq 4$.

Proof. (a) Set $p = k_1$. Choose some $1 < i < j < p$ (notice that $p \geq 4$). By (3)

$$(1\,2 \cdots p) \cdot (1\; i)(j\; p) = (1\; i+1 \cdots j)(2 \cdots i)(j+1 \cdots p).$$

By choosing $i = p' + 1$ and $j = p' + p'''$, we obtain a (p''', p', p'')-cycle.

(b1) Set $p = k_1$ and $q = k_2$. Choose $1 \le i < j \le p$ such that $j - i = p'$ and $p+1 \le k < m \le p+q$ such that $m-k = q'$ and apply (3) to

$$(1\,2 \cdots p)(p+1 \cdots p{+}q) \cdot (i\ j)(k\,m).$$

(b2) Set $p = k_1$ and $q = k_2$. Choose $1 \le i < j \le p+q$ distinct from $p, p+q$ (notice that $p+q \ge 4$ by assumption). By (4) and (3)

$$(1\,2 \cdots p)(p+1 \cdots p{+}q) \cdot (p\ p{+}q)(i\ j) = (1\,2 \cdots p{+}q) \cdot (i\ j)$$

is a product of two cycles of lengths $j-i$ and $p+q-j+i$. If we choose $i = 1$ and $2 \le j \le p-1$ we obtain a $(p', p{+}q{-}p')$-cycle for any $1 \le p' \le p-2$. If $p \ge 3$ and $q \ge 2$ we may choose $i = 2$ and $j = p+1$ to get a $(p{-}1, q{+}1)$-cycle.

(c1) Set $p = k_1 \ge 2$ and $q = k_2$ and $t = k_3$. Check that

$$(1 \cdots p)(p+1 \cdots p{+}q)(p{+}q{+}1 \cdots p{+}q{+}t) \cdot (p\ p{+}q)(1\ p{+}q{+}t)$$

is a $p{+}q{+}t$-cycle (use (4)).

(c2) Set $p = k_1$ and $q = k_2$ and $t = k_3$. For any $1 \le i < p$ (note that $p \ge 2$)

$$(1 \cdots p)(p+1 \cdots p{+}q)(p{+}q{+}1 \cdots p{+}q{+}t) \cdot (i\ p)(p{+}q\ p{+}q{+}t)$$

is a $(i, p{-}i, q{+}t)$-cycle (use (3) and (4)).

(d) If $\alpha_1\alpha_2\beta_1\beta_2$ is a product of disjoint cycles (possibly of length 1), use (4) twice to get an $\alpha\beta$ product of disjoint cycles of lengths $|\alpha_1| + |\alpha_2|$ and $|\beta_1| + |\beta_2|$. □

Notation 4.11. In light of the discussion in 4.8, the cases of Proposition 4.9 will be referred to O_3(a), O_3(b) and O_3(c) and those of Proposition 4.10 as O_2(a), O_2(b1), O_2(b2) etc. This reminds us that we view 3-cycles and (2, 2)-cycles as "operations" on permutations which either split or fuse cycles.

Lemma 4.12. *Consider $\sigma \in S_n$ with cycle structure $[k_1, \dots, k_r]$, where $k_i \ge 1$ and $\sum_i k_i = n$. Let $1 \le m \le n$. Then there exist $\ell \ge 0$ and 3-cycles $\alpha_1, \dots, \alpha_\ell$ such that $r \ge 2\ell + 1$ and if we set $\tilde{k} = \sum_{i=1}^{2\ell+1} k_i$ then the cycle structure of $\sigma\alpha_1 \cdots \alpha_\ell$ is either*

(i) $[\tilde{k}, k_{2\ell+2}]$, *where $r = 2\ell + 2$ and $\tilde{k} \le m-1$, or*

(ii) $[\tilde{k}, k_{2\ell+2}, \dots, k_r]$ *and $\tilde{k} \ge m$ and $\sum_{i=1}^{2\ell-1} k_i < m$.*

In fact, for any $0 \le j \le \ell$ the cycle structure of $\sigma\alpha_1 \cdots \alpha_j$ is

$$\left[\sum_{i=1}^{2j+1} k_i, k_{2j+2}, \dots, k_r\right].$$

(*Notice that in* (ii) *it may happen that $r = 2\ell + 1$; hence $\tilde{k} = n$ and $\sigma\alpha_1 \cdots \alpha_{2\ell+1}$ is an n-cycle*).

Proof. Apply O_3(c) repeatedly to choose 3-cycles $\alpha_1, \dots, \alpha_\ell$ that "fuse" the first cycle with the next two until the first instance when $\sum_{i=1}^{2\ell+1} k_i \ge m$ or until $\sigma\alpha_1 \cdots \alpha_\ell$ contains only one or two cycles (If there are three or more cycles left and $\sum_{i=1}^{2\ell+1} k_i < m$, we will proceed applying O_3(c)). In the first two cases we have established (ii) (since $\sum_i k_i = n \ge m$) and in the third case (two cycles remaining) it is (i). □

Proposition 4.13. *Let $\tau \in S_n$ be an odd permutation. Suppose that τ contains a k-cycle, where $k \ge 3$ is odd and that $n - k \ge 2$. Then*

$$\|S_n\|_\tau \le \Delta(S_{n-k}) + k.$$

Proof. By assumption $n \ge k + 2 \ge 5$. Let $\sigma \in S_n$ be a nonidentity element. Our goal is to prove that $\|\sigma\|_\tau \le \Delta(S_{n-k}) + k$. We will do this in three steps.

Step I: There are 3-cycles $\alpha_1, \dots, \alpha_t$, where $t \le \frac{k-1}{2}$ such that $\sigma\alpha_1 \cdots \alpha_t$ contains a k-cycle.

Proof of Step I. Let $[k_1, \dots, k_r]$ be the cycle structure of σ, where $\sum_i k_i = n$ and $k_1 \ge \cdots \ge k_r$. Note that $k_1 \ge 2$ since $\sigma \ne \mathrm{id}$. Recall Notation 4.11.

If σ is a transposition, its cycle structure is $[1, \dots, 1, 2]$, with $n - 2 \ge k$ fixed points. Apply O_3(c) repeatedly $t = \frac{k-1}{2}$ times with 3-cycles $\alpha_1, \dots, \alpha_t$ to obtain $\sigma\alpha_1 \cdots \alpha_t \in [k, 1, \dots, 1, 2]$ and we are done.

Assume that σ is not a transposition. Then either $k_1 \ge 3$ or $k_1, k_2 \ge 2$. Hence, if $r \ge 2$ then $k_1 + k_2 \ge 4$.

Use Lemma 4.12 with $m = k$ to find 3-cycles $\alpha_1, \dots, \alpha_\ell$ such that $\ell \ge 0$ and $r \ge 2\ell + 1$ and if we set $\tilde{k} = \sum_{i=1}^{2\ell+1} k_i$ then the cycle structure of $\xi = \sigma\alpha_1 \cdots \alpha_\ell$ is either

(i) $[\tilde{k}, k_{2\ell+2}]$, where $\tilde{k} \le k - 1$, or

(ii) $[\tilde{k}, k_{2\ell+2}, \dots, k_r]$, where $\tilde{k} \ge k$ and $\sum_{i=1}^{2\ell-1} k_i < k$.

Case (i): We have $\xi \in [\tilde{k}, n - \tilde{k}]$, where $\tilde{k} < k$. Use O_3(b) to find a 3-cycle $\alpha_{\ell+1}$ such that $\xi\alpha_{\ell+1} \in [k, n - k]$ contains a k-cycle. It remains to show that $\ell + 1 \le \frac{k-1}{2}$. If $\ell = 0$ then we are done. If $\ell \ge 1$ then $r \ge 3$ and

$$k_1 + k_2 + \sum_{i=3}^{2\ell+1} k_i = \sum_{i=1}^{2\ell+1} k_i \le k - 1.$$

Since $k_1 + k_2 \ge 3$ and $k_i \ge 1$ we get $3 + 2\ell - 1 \le k - 1$ so $\ell \le \frac{k-3}{2}$ and we are done.

Case (ii): If $\tilde{k} = k$ then ξ contains a k-cycle. If $\tilde{k} = k+1$ then $r \ge 2\ell+2$ since $n > k+1$ and we use O_3(b) to find a 3-cycle $\alpha_{\ell+1}$ such that $\xi\alpha_{\ell+1} \in [k, \tilde{k} + k_{2\ell+2} - k, \dots, k_r]$ contains a k-cycle. If $\tilde{k} \ge k + 2$, use O_3(a) to find a 3-cycle $\alpha_{\ell+1}$ such that $\xi\alpha_{\ell+1} \in [k, 1, \tilde{k} - k - 1, \dots]$ contains a k-cycle. Thus, a product of σ with at most $\ell + 1$ 3-cycles gives a permutation which contains a k-cycle.

If $\ell = 0$ then $\ell+1 = 1 \le \frac{k-1}{2}$ and we are done. If $\ell \ge 2$ then $r \ge 5$ and

$$\sum_{i=1}^{2\ell-1} k_i = k_1 + k_2 + \sum_{i=3}^{2\ell-1} k_i \ge 4 + (2\ell-3).$$

By assumption $\sum_{i=1}^{2\ell-1} k_i \le k-1$ so $\ell \le \frac{k-2}{2}$ and since k is odd, $\ell \le \frac{k-3}{2}$. Therefore $\ell+1 \le \frac{k-1}{2}$ and we are done.

It remains to consider the case $\ell = 1$. If $k \ge 5$ then $\ell+1 \le \frac{k-1}{2}$ and we are done. Assume $k = 3$. By assumption $k_1 = \sum_{i=1}^{2\ell-1} k_i \le k-1 = 2$. Then $k_2 \le k_1 \le 2$ and since σ is not a transposition, $k_2 = 2$; namely $\sigma \in [2, 2, \dots]$. Use O_3(b) to replace α_1 with a 3-cycle so that $\sigma\alpha_1 \in [3, 1, \dots]$ and we are done $\big($since $1 \le \frac{k-1}{2}\big)$. This completes the proof of Step I. □

Step II: If $\mu \in S_n$ contains a k-cycle then $\|\mu\|_\tau \le \Delta(S_{n-k}) + 1$.

Proof of Step II. Write $\mu = \mu_0\mu_k$ as a product of disjoint permutations, where $\mu_k \in S_k$ is a k-cycle and $\mu_0 \in S_{n-k}$. By assumption $n-k \ge 2$. Similarly, $\tau = \tau_0\tau_k$. Since τ is an odd permutation and τ_k is an even permutation (a cycle of odd length), τ_0 is an odd permutation in S_{n-k} and by Lemma 4.4 it normally generates it. By Lemma 4.2 there are $\lambda_1, \dots, \lambda_\ell \in S_{n-k}$, where $\ell \le \Delta(S_{n-k})$, such that

$$\mu_0 = \tau_0^{\lambda_1} \cdots \tau_0^{\lambda_\ell}.$$

Choose $\theta \in S_k$ such that $\tau_k^\theta = \tau_k^{-1}$. Since k is odd, τ_k^2 is a k-cycle, so there is $\pi \in S_k$ such that $\tau_k^\pi = \tau_k^2$.

If ℓ is odd then

$$\tau^{\lambda_1}\tau^{\lambda_2\theta}\tau^{\lambda_3}\tau^{\lambda_4\theta}\cdots\tau^{\lambda_{\ell-2}}\tau^{\lambda_{\ell-1}\theta}\tau^{\lambda_\ell} = (\tau_0^{\lambda_1}\cdots\tau_0^{\lambda_\ell}) \cdot ((\tau_k\tau_k^\theta)^{(\ell-1)/2} \cdot \tau_k) = \mu_0\tau_k$$

is conjugate to μ (since both μ_k and τ_k are k-cycles) so $\|\mu\|_\tau \le \ell \le \Delta(S_{n-k})$.

Assume that ℓ is even. If $\ell = 0$ then $\mu = \mu_k$ is a k-cycle. Choose some $\epsilon \in S_{n-k}$ such that $\tau_0^\epsilon = \tau_0^{-1}$ and then

$$\tau^\epsilon \cdot \tau = (\tau_0^\epsilon\tau_0) \cdot (\tau_k^2) = \tau_k^2$$

is a k-cycle, and hence is conjugate to μ. Now, $n-k \ge 2$ so $\|\mu\|_\tau = 2 \le \Delta(S_{n-k})+1$ by Corollary 4.6 as needed. If $\ell \ge 2$ then

$$\begin{aligned}\tau^{\lambda_1\pi}\tau^{\lambda_2\theta}\tau^{\lambda_3}\tau^{\lambda_4\theta}\tau^{\lambda_5}\cdots\tau^{\lambda_{\ell-1}}\tau^{\lambda_\ell\theta} &= (\tau_0^{\lambda_1}\cdots\tau_0^{\lambda_\ell}) \cdot (\tau_k^\pi\tau_k^\theta\tau_k\tau_k^\theta\cdots\tau_k\tau_k^\theta) \\ &= \mu_0 \cdot (\tau_k^2\tau_k^{-1} \cdot (\tau_k\tau_k^{-1})^{(\ell-2)/2}) = \mu_0\tau_k\end{aligned}$$

is conjugate to μ so $\|\mu\|_\tau \le \ell \le \Delta(S_{n-k})$. This completes the proof of Step II. □

Step III: We show that $\|\sigma\|_\tau \le \Delta(S_{n-k}) + k$.

Proof of Step III. By Step I there are 3-cycles $\alpha_1, \dots, \alpha_t$, where $t \leq \frac{k-1}{2}$, such that $\mu = \sigma\alpha_1 \cdots \alpha_t$ contains a k-cycle. By Step II, $\|\mu\|_\tau \leq \Delta(S_{n-k}) + 1$. Since τ contains a k-cycle of length $k \geq 3$, Lemma 4.7 shows that $\|\alpha_i\|_\tau \leq 2$. Therefore

$$\|\sigma\|_\tau \leq \|\mu\|_\tau + \sum_{i=1}^{t} \|\alpha_i^{-1}\|_\tau \leq \Delta(S_{n-k}) + 1 + 2t \leq \Delta(S_{n-k}) + k. \qquad \square$$

There are three (2, 2)-cycles in S_4, and the product of any two is equal to the third. Therefore if τ is a (2, 2)-cycle in S_n there exists $\pi \in S_n$ such that $\mathrm{supp}(\pi) \subseteq \mathrm{supp}(\tau)$ and $\tau^\pi \tau$ is a (2, 2)-cycle.

Proposition 4.14. *Let $\tau \in S_n$ be an odd permutation, $n \geq 7$. Suppose that τ contains a (p, q)-cycle, where $p \geq q \geq 2$ are even and $n - (p + q) \geq p$. Then*

$$\|S_n\|_\tau \leq \Delta(S_{n-(p+q)}) + p + q.$$

Proof. We will prove that if $1 \neq \sigma \in S_n$ then $\|\sigma\|_\tau \leq \Delta(S_{n-(p+q)}) + p + q$. Throughout the proof the cycle structure of σ is $[k_1, \dots, k_r]$ such that $k_i \geq 1$ and $\sum_i k_i = n$ and $k_1 \geq \cdots \geq k_r$. Recall Notation 4.11.

Step I: There exist $\alpha_1, \dots, \alpha_t \in S_n$ such that $t \leq \frac{p+q-2}{2}$ and such that $\xi = \sigma\alpha_1 \cdots \alpha_t$ contains a (p, q)-cycle and the following hold. If $p = 2$ then every α_i is a (2, 2)-cycle and if $p \geq 4$ then each α_i is either a 3-cycle or a (2, 2)-cycle.

Proof of Step I. Assume first that $p = 2$. Hence, $q = 2$. If $k_1 \geq 5$ then use O_2(a) to find a (2, 2)-cycle α_1 such that $\sigma\alpha_1 \in [2, k_1 - 4, 2, \dots]$, i.e., $\sigma\alpha_1$ contains a (2, 2)-cycle, and we are done (since $t = 1 \leq \frac{p+q-2}{2} = 1$).

If $k_1, k_2 \geq 3$ then use O_2(b1) to find a (2, 2)-cycle α_1 such that $\sigma\alpha_1 \in [2, k_1 - 2, 2, k_2 - 2, \dots]$ and we are done.

If $k_1 = 4$ and $k_2 = 2$ then use O_2(b1) to find a (2, 2)-cycle α_1 such that $\sigma\alpha_1 \in [2, 2, 1, 1, \dots]$. If $k_1 = 4$ and $k_2 = 1$ then $r \geq 3$ and $k_3 = 1$ (since $n \geq 7$) and we use O_2(c2) to get $\sigma\alpha_1 \in [2, 2, 2, \dots]$ and we are done.

Suppose that $k_1 = 3$ and $k_2 = 2$. Then $r \geq 3$ since $n \geq 7$. If $k_3 = 2$ then σ contains a (2, 2)-cycle and we are done. Otherwise $k_3 = 1$. Then $r \geq 4$ since $n \geq 7$ and $\sigma \in [3, 2, 1, 1, \dots] = [3, 1, 1, 2, \dots]$ and we use O_2(c2) to find a (2, 2)-cycle α_1 such that $\sigma\alpha_1 \in [2, 1, 2, 2, \dots]$ and we are done.

If $k_1 = 3$ and $k_2 = 1$ then $r \geq 4$ and $k_3 = 1$ and use O_2(c2) to get $\sigma\alpha_1 \in [2, 1, 2, \dots]$ and we are done.

If $k_1 = 2$ and $k_2 = 2$ then σ contains a $(2, 2)$-cycle we are done. If $k_1 = 2$ and $k_2 = 1$ then σ is a transposition which fixes at least four points (since $n \geq 6$) and we can use them to choose a $(2, 2)$-cycle α_1 supported by $\mathrm{fix}(\sigma)$ and then $\sigma\alpha_1 \in [2, 2, 2]$ and we are done. This completes the proof of Step I in the case $p = 2$.

For the remainder of the proof $p \geq 4$. In particular $p+q \geq 6$. Assume first that σ is a transposition. We may assume that $\operatorname{supp}(\sigma) = \{n-1, n\}$ and notice that $n-2 \geq p+q$ by the assumption. Choose a $(2,2)$-cycle $\alpha_0 \in S_{n-2}$ arbitrarily. Use O_3(c) $\frac{p-2}{2}$ times to find 3-cycles $\beta_1, \dots, \beta_{(p-2)/2} \in S_{n-2}$ such that $\theta = \alpha_0\beta_1 \cdots \beta_{(p-2)/2}$ is a $(p,2)$-cycle. Use O_3(c) $\frac{q-2}{2}$ times to find 3-cycles $\gamma_1, \dots, \gamma_{(q-2)/2} \in S_{n-2}$ such that $\theta\gamma_1, \dots, \gamma_{(q-2)/2}$ is a (p,q)-cycle. Then

$$\sigma\alpha_0\beta_1 \cdots \beta_{(p-2)/2}\gamma_1 \cdots \gamma_{(q-2)/2} \in [p, q, 2]$$

and we are done since $\frac{p-2}{2} + \frac{q-2}{2} + 1 = \frac{p+q-2}{2}$.

Therefore for the remainder of the proof of Step I we assume that σ is not a transposition. Hence, if $r \geq 2$ then $k_1 + k_2 \geq 4$.

Use Lemma 4.12 with $m = p+q+1$ to find 3-cycles $\alpha_1, \dots, \alpha_\ell$, where $\ell \geq 0$ and $r \geq 2\ell+1$ such that if we set $\tilde{k} = \sum_{i=1}^{2\ell+1} k_i$ and $\xi = \sigma\alpha_1 \cdots \alpha_\ell$ then either

(i) $\tilde{k} \leq p+q$ and $r = 2\ell+2$ and $\xi \in [\tilde{k}, k_{2\ell+2}]$, or

(ii) $\tilde{k} \geq p+q+1$ and $\sum_{i=1}^{2\ell-1} k_i \leq p+q$ and $\xi \in [\tilde{k}, k_{2\ell+2}, \dots, k_r]$.

Case (i): Observe that $k_{2\ell+2} = n - \tilde{k} \geq n - (p+q) \geq p \geq 4$. Therefore $k_i \geq 4$ for all i and therefore

$$p+q \geq \sum_{i=1}^{2\ell+1} k_i \geq 4(2\ell+1).$$

It follows that $\ell \leq \lfloor \frac{p+q-4}{8} \rfloor$.

Since $\xi \in [\tilde{k}, n-\tilde{k}]$, use O_3(b) to find a 3-cycle $\alpha_{\ell+1}$ such that $\xi\alpha_{\ell+1} \in [n-1, 1]$. Since $n-1 > p+q$, use O_3(a) to find a 3-cycle $\alpha_{\ell+2}$ such that $\xi\alpha_{\ell+1}\alpha_{\ell+2} \in [p, q, n-1-p-q]$ contains a (p,q)-cycle. We are done because $\ell+2 \leq \lfloor \frac{p+q+12}{8} \rfloor$ and one checks that $\lfloor \frac{p+q+12}{8} \rfloor \leq \frac{p+q-2}{2}$ if $p+q \geq 6$.

Case (ii): If $\ell = 0$ then $\sigma = [k_1, \dots]$, where $k_1 \geq p+q+1$. Then use O_3(a) to find a 3-cycle α_1 such that $\sigma\alpha_1 \in [p, q, k_1 - p - q, \dots]$ and we are done $\big($since $1 \leq \frac{p+q-2}{2}\big)$. So we only need to consider $\ell \geq 1$.

Suppose first that $\sum_{i=1}^{2\ell-1} k_i = p+q$. Then $\sigma\alpha_1 \cdots \alpha_{\ell-1} \in [p+q, k_{2\ell}, k_{2\ell+1}, \dots]$. Use O_2(c2) to replace α_ℓ with a $(2,2)$-cycle such that $\sigma\alpha_1 \cdots \alpha_\ell \in [p, q, k_{2\ell} + k_{2\ell+1}, \dots]$. If $\ell = 1$ then $\ell \leq \frac{p+q-2}{2}$ and we are done. If $\ell \geq 2$ then

$$p+q = \sum_{i=1}^{2\ell-1} k_i = k_1 + k_2 + \sum_{i=3}^{2\ell-1} k_i \geq 4 + 2\ell - 3$$

since $k_i \geq 1$. Therefore $\ell \leq \lfloor \frac{p+q-1}{2} \rfloor = \frac{p+q-2}{2}$ since $p+q$ is even, and we are done.

It remains to consider the case $\sum_{i=1}^{2\ell-1} k_i \leq p+q-1$. Assume first that $k_{2\ell} = 1$. This implies that $k_{2\ell+1} = 1$ and since $\sum_{i=1}^{2\ell+1} k_i \geq p+q+1$ it follows that $\sum_{i=1}^{2\ell} k_i =$

$p+q$, and therefore $\sigma\alpha_1\cdots\alpha_{\ell-1}\in[p+q-1,1,1,\dots]$. Use O_3(b) to replace α_ℓ with a 3-cycle such that $\sigma\alpha_1\cdots\alpha_\ell\in[p,q,1,\dots]$. Since $k_1\geq 2$ and $k_i\geq 1$ we get

$$p+q=\sum_{i=1}^{2\ell}k_i\geq 2+2\ell-1$$

and therefore $\ell\leq\lfloor\frac{p+q-1}{2}\rfloor=\frac{p+q-2}{2}$ and we are done.

Assume that $k_{2\ell}\geq 2$. Since $\tilde{k}\geq p+q+1$, use O_3(a) to find a 3-cycle $\alpha_{\ell+1}$ such that $\xi\alpha_{\ell+1}\in[p,q,\tilde{k}-p-q,\dots]$ contains a (p,q)-cycle. Since $k_1\geq\cdots\geq k_{2\ell}\geq 2$ and $\sum_{i=1}^{2\ell-1}k_i\leq p+q-1$ we deduce that $2(2\ell-1)\leq p+q-1$; hence $\ell\leq\lfloor\frac{p+q+1}{4}\rfloor=\frac{p+q}{4}$. Therefore $\ell+1\leq\lfloor\frac{p+q+4}{4}\rfloor$ and we are done since $\lfloor\frac{p+q+4}{4}\rfloor\leq\frac{p+q}{2}$ if $p+q\geq 6$. This completes the proof of Step I. □

Step II: Let $\mu\in S_n$ contain a (p,q)-cycle. Then $\|\mu\|_\tau\leq\Delta(S_{n-p-q})+2$.

Proof of Step II. We first consider the case $p=2$. Hence $q=2$. Consider $\mu\in S_n$, which contains a $(2,2)$-cycle. We write μ as a product of disjoint permutations $\mu=\mu_0\mu_{2,2}$, where $\mu_{2,2}$ is a $(2,2)$-cycle in S_4 and $\mu_0\in S_{n-4}$. Notice that $n-4=n-(p+q)\geq p=2$. Similarly we write $\tau=\tau_0\tau_{2,2}$. Since τ is an odd permutation and $\tau_{2,2}$ is even, $\tau_0\in S_{n-4}$ is an odd permutation, and by Lemma 4.4 it normally generates it. By Lemma 4.2 there are $\lambda_1,\dots,\lambda_\ell\in S_{n-4}$, where $\ell\leq\Delta(S_{n-4})$ such that

$$\mu_0=\tau_0^{\lambda_1}\cdots\tau_0^{\lambda_\ell}.$$

Suppose that ℓ is odd. Since $|\tau_{2,2}|=2$,

$$\tau^{\lambda_1}\cdots\tau^{\lambda_\ell}=(\tau_0^{\lambda_1}\cdots\tau_0^{\lambda_\ell})\cdot(\tau_{2,2})^\ell=\mu_0\tau_{2,2}$$

is conjugate to μ since both $\mu_{2,2}$ and $\tau_{2,2}$ are $(2,2)$-cycles, so $\|\mu\|_\tau\leq\ell\leq\Delta(S_{n-4})$.

Suppose that ℓ is even. If $\ell=0$ then $\mu=\mu_{2,2}$ is $(2,2)$-cycle. Since τ contains a $(2,2)$-cycle, $\|\mu\|_\tau\leq 2\leq\Delta(S_{n-4})+2$ and we are done. Otherwise $\ell\geq 2$. In this case we choose $\pi\in S_4$ such that $\tau_{2,2}^\pi\tau_{2,2}$ is a $(2,2)$-cycle. Then

$$\tau^{\lambda_1\pi}\tau^{\lambda_2}\cdots\tau^{\lambda_\ell}=(\tau_0^{\lambda_1}\cdots\tau_0^{\lambda_\ell})\cdot(\tau_{2,2}^\pi\tau_{2,2}\cdot(\tau_{2,2})^{\ell-2})=\mu_0\cdot(\tau_{2,2}^\pi\tau_{2,2})$$

is conjugate to μ; hence $\|\mu\|_\tau\leq\ell\leq\Delta(S_{n-4})$ and this completes the proof of Step II in the case $p=2$.

For the remainder of the proof of Step II assume $p\geq 4$. Write $\mu=\mu_0\mu_{p,q}$, a product of disjoint permutations with $\mu_{p,q}\in S_{p+q}$ a (p,q)-cycle and $\mu_0\in S_{n-p-q}$. Notice that $n-p-q\geq p\geq 4$ by assumption. Similarly write $\tau=\tau_0\tau_{p,q}$. Since τ is odd and $\tau_{p,q}$ is even, τ_0 is odd and therefore normally generates S_{n-p-q}. By Lemma 4.2 there are $\lambda_1,\dots,\lambda_\ell\in S_{n-p-q}$, where $\ell\leq\Delta(S_{n-p-q})$, such that

$$\mu_0=\tau_0^{\lambda_1}\cdots\tau_0^{\lambda_\ell}.$$

Choose $\theta\in S_{p+q}$ such that $\tau_{p,q}^\theta=\tau_{p,q}^{-1}$.

If ℓ is odd then

$$\tau^{\lambda_1}\tau^{\lambda_2\theta}\tau^{\lambda_3}\tau^{\lambda_4\theta}\cdots\tau^{\lambda_{\ell-1}\theta}\tau^{\lambda_\ell} = (\tau_0^{\lambda_1}\cdots\tau_0^{\lambda_\ell})\cdot((\tau_{p,q}\tau_{p,q}^{-1})^{(\ell-1)/2}\cdot\tau_{p,q}) = \mu_0\tau_{p,q}$$

is conjugate to μ so $\|\mu\|_\tau \le \ell \le \Delta(S_{n-p-q})$.

Suppose that ℓ is even. Since both p, q are even, $\tau_{p,q}^2$ is a $\left(\frac{p}{2}, \frac{p}{2}, \frac{q}{2}, \frac{q}{2}\right)$-cycle. Use O_2(d) to find a $(2, 2)$-cycle β such that $\tau_{p,q}\beta$ is a (p, q)-cycle.

If $\ell = 0$ then $\mu = \mu_{p,q}$. Choose $\pi \in S_{n-p-q}$ such that $\tau_0^\pi = \tau_0^{-1}$. Then

$$\tau\tau^\pi\beta = (\tau_0\tau_0^{-1})(\tau_{p,q}^2)\beta \in [p, q]$$

is conjugate to μ. Since $p \ge 4$, Lemma 4.7 gives $\|\beta\|_\tau \le 2$ and therefore $\|\mu\| \le \|\tau\|_\tau + \|\tau^\pi\|_\tau + \|\beta\|_\tau \le 4$. By Corollary 4.6 and since $n - p - q \ge p \ge 4$, we get $\Delta(S_{n-p-q}) + 2 \ge 3 + 2 > \|\mu\|_\tau$.

If $\ell \ge 2$ is even then

$$\begin{aligned}\tau^{\lambda_1}\tau^{\lambda_2}\tau^{\lambda_3\theta}\tau^{\lambda_4}\tau^{\lambda_5\theta}\tau^{\lambda_6}\cdots\tau^{\lambda_{\ell-1}\theta}\tau^{\lambda_\ell}\cdot\beta &= (\tau_0^{\lambda_1}\cdots\tau_0^{\lambda_\ell})\cdot(\tau_{p,q}^2(\tau_{p,q}^{-1}\tau_{p,q})^{(\ell-2)/2})\cdot\beta \\ &= \mu_0\cdot\tau_{p,q}^2\cdot\beta\end{aligned}$$

is conjugate to μ since $\tau_{p,q}^2\beta$ is a (p, q)-cycle. Therefore

$$\|\mu\|_\tau \le \ell + \|\beta\|_\tau = \ell + 2 \le \Delta(S_{n-p-q}) + 2.$$

This completes the proof of Step II. □

Step III: We prove that $\|\sigma\|_\tau \le \Delta(S_{n-p-q}) + p + q$.

Proof of Step III. First, consider the case $p = 2$. Hence $q = 2$. By Step I there are $(2, 2)$-cycles $\alpha_1, \ldots, \alpha_t$ where $t \le \frac{p+q-2}{2}$ such that $\mu = \sigma\alpha_1\cdots\alpha_t$ contains a (p, q)-cycle. By Step II, $\|\mu\|_\tau \le \Delta(S_{n-p-q}) + 2$. By Lemma 4.7, $B_\tau(2)$ contains all $(2, 2)$-cycles. Therefore

$$\|\sigma\|_\tau \le \|\mu\|_\tau + 2t \le \Delta(S_{n-p-q}) + 2 + (p + q - 2) = \Delta(S_{n-p-q}) + p + q.$$

If $p \ge 4$ then Lemma 4.7 implies that $B_\tau(2)$ contains all 3-cycles and all $(2, 2)$-cycles. By Step I there are $\alpha_1, \ldots, \alpha_t$ such that $t \le \frac{p+q-2}{2}$ and α_i are either 3-cycles or $(2, 2)$-cycles and $\mu = \sigma\alpha_1\cdots\alpha_t$ contains a (p, q)-cycle. By Step II $\|\mu\|_\tau \le \Delta(S_{n-p-q}) + 2$ so

$$\|\sigma\|_\tau \le \|\mu\|_\tau + 2t \le \Delta(S_{n-p-q}) + 2 + (p + q - 2) = \Delta(S_{n-p-q}) + p + q. \quad \square$$

Proposition 4.15. *Let $\tau \in S_n$ be an n-cycle, $n \ge 4$ even. Then $\|S_n\|_\tau \le n - 1$.*

Proof. First, τ is an odd permutation, and hence normally generates S_n by Lemma 4.4. Since $n \ge 4$, Lemma 4.7 shows that $B_\tau(2)$ contains all 3-cycles and all $(2, 2)$-cycles. Consider some $1 \ne \sigma \in S_n$ with cycle structure $[k_1, \ldots, k_r]$, where $\sum_i k_i = n$ and $k_1 \ge \cdots \ge k_r$. Then $k_1 \ge 2$ since $\sigma \ne 1$. We need to show that $\|\sigma\|_\tau \le n - 1$.

Suppose first that r is odd. If $r = 1$ then σ is an n-cycle, $\|\sigma\|_\tau = 1 \le n-1$ and we are done. If $r \ge 3$, use O_3(a) to find a 3-cycle α_1 such that $\sigma\alpha_1 \in [k_1, k_2, k_3, n-(k_1+k_2+k_3)]$. Repeat this process to find 3-cycles $\alpha_2, \dots, \alpha_{(r-1)/2}$ such that $\sigma\alpha_1 \cdots \alpha_{(r-1)/2} \in [k_1, \dots, k_r]$ (this is possible since r is odd). This shows that

$$\|\sigma\|_\tau \le \tfrac{r-1}{2} \cdot \|\alpha_i\|_\tau \le 2 \cdot \tfrac{r-1}{2} = r-1 \le n-1.$$

Suppose that r is even ($r \ge 2$). Then σ is not a transposition (because in that case r is odd). If σ is either a 3-cycle or a $(2,2)$-cycle then $\|\sigma\|_\tau \le 2$ by Lemma 4.7 and we are done since $n \ge 4$. Therefore either

- $k_1 \ge 4$, in which case $r \le 1 + (n - k_1) \le n-3$, or
- $k_1 = 3$ and $k_2 \ge 2$ in which case $r \le 1 + 1 + (n-5) = n-3$, or
- $k_1 = 2$ and $k_2, k_3 = 2$ (since σ is not a transposition nor a $(2,2)$-cycle), so $r \le 3 + (n-6) = n-3$.

So we may assume that $r \le n-3$.

Since n is even, τ^2 is an $\left(\frac{n}{2}, \frac{n}{2}\right)$-cycle. Since $k_1 \ge \cdots \ge k_r$ and $r \ge 2$ and $\sum_i k_i = n$, we see that $k_r \le \frac{n}{2}$. If $k_r = \frac{n}{2}$ then $r = 2$ and σ is an $\left(\frac{n}{2}, \frac{n}{2}\right)$-cycle, so

$$\|\sigma\|_\tau = \|\tau^2\|_\tau = 2 \le n-1$$

and we are done. So assume $k_r < \frac{n}{2}$. Apply O_3(b) to τ^2 to find a 3-cycle α_0 such that $\tau^2\alpha_0 \in [n-k_r, k_r]$. Apply O_3(a) $\frac{r-2}{2}$ times to find 3-cycles $\alpha_1, \dots, \alpha_t$, where $t = \frac{r-2}{2}$, that split the $(n-k_r)$-cycle into $r-1$ cycles and get $\sigma\alpha_0 \cdots \alpha_t \in [k_1, \dots, k_r]$. Since $\|\alpha_i\|_\tau \le 2$ we get

$$\|\sigma\|_\tau \le 2(t+1) = r \le n-1$$

(because $\sigma \ne 1$). □

Proposition 4.16. *Consider an odd permutation $\tau \in S_n$ and assume that τ fixes a point. Then $\|S_n\|_\tau \le \|S_{n-1}\|_\tau + 1$. In particular $\|S_n\|_\tau \le \Delta(S_{n-1}) + 1$.*

Proof. Up to conjugation we may assume that τ fixes n. Any $\sigma \in S_n$ either fixes a point, in which case up to conjugacy $\sigma \in S_{n-1}$, or there exists τ' conjugate to τ such that $\sigma\tau'$ fixes a point. So up to conjugation $\sigma\tau' \in S_{n-1}$ for some $\tau' \in B_\tau(1)$. Therefore

$$\|\sigma\|_\tau \le \|\sigma\tau'\|_\tau + \|\tau'\|_\tau \le \|S_{n-1}\|_\tau + 1 \le \Delta(S_{n-1}) + 1.$$ □

Proof of Theorem 1.2. We use induction on $n \ge 2$. First, $\Delta(S_2) = 1$ is a triviality and $\Delta(S_3) = 2$ by Theorem 1.1.

Assume inductively that $\Delta(S_m) = m-1$ for all $2 \le m < n$. By Corollary 4.6, $\Delta(S_n) \ge n-1$. To prove equality we need to show that $\|S_n\|_X \le n-1$ for any normally generating set X. By Lemma 4.4, X contains an odd permutation τ which normally generates, and hence $\|S_n\|_X \le \|S_n\|_\tau$. So it suffices to prove that $\|S_n\|_\tau \le n-1$ for any odd permutation τ.

If τ has a fixed point then by Proposition 4.16

$$\|S_n\|_\tau \le \Delta(S_{n-1}) + 1 \le n-2+1 = n-1$$

and we are done. So in order to establish the induction step we need to check that $\|S_n\|_\tau \le n-1$ for odd τ without fixed points. Recall Notation 4.11.

For $n = 4$ the only fixed-point free odd permutations are the 4-cycles. If τ is one then $\|S_4\|_\tau \le 3$ by Proposition 4.15. So $\Delta(S_4) = 3$.

For $n = 5$ the only fixed-point free odd permutations are the $(3, 2)$-cycles. Let τ be one. Then $[3, 2] \subseteq B_\tau(1)$ by definition and $[3] \subseteq B_\tau(2)$ by Lemma 4.7. We apply Proposition 2.2(iii) and O_3(a) to deduce that

$$[2] = [1, 1, 1, 2] \subseteq [3, 2] \cdot [3] \subseteq B_\tau(3)$$

and O_3(b) to deduce that

$$[4] = [1, 4] \subseteq [3, 2] \cdot [3] \subseteq B_\tau(3).$$

Apply O_3(b) to get

$$[2, 2] \subseteq [3, 1] \cdot [3] \subseteq B_\tau(4)$$

and O_3(c) to get

$$[5] \subseteq [3, 1, 1] \cdot [3] \subseteq B_\tau(4).$$

We have exhausted all the nontrivial conjugacy classes in S_5 and therefore $\|S_5\|_\tau \le 4$ as needed.

For $n = 6$ the only fixed-point free odd permutations are the $(2, 2, 2)$-cycles and 6-cycles. If τ is a 6-cycle then $\|S_6\|_\tau \le 5$ by Proposition 4.15. Consider $\tau \in [2, 2, 2]$. Then $[2, 2, 2] \subseteq B_\tau(1)$ by definition and $[2, 2] \subseteq B_\tau(2)$ by Lemma 4.7. Now, $[2], [6], [4] \subseteq B_\tau(3)$ because

$$\begin{aligned} &[2] = [1, 1, 1, 1, 2] \subseteq [2, 2, 2] \cdot [2, 2] && \text{by } O_2(\text{b1}),\\ &[6] \subseteq [2, 2, 2] \cdot [2, 2] && \text{by } O_2(\text{c1}),\\ &[4] = [1, 1, 4] \subseteq [2, 2, 2] \cdot [2, 2] && \text{by } O_2(\text{c2}). \end{aligned}$$

Next, $[5], [3], [4, 2], [3, 3] \subseteq B_\tau(4)$ because

$$\begin{aligned} &[5] \subseteq [2, 2, 1] \cdot [2, 2] && \text{by } O_2(\text{c1}),\\ &[3] = [1, 1, 3] \subseteq [2, 2, 1] \cdot [2, 2] && \text{by } O_2(\text{c2}),\\ &[4, 2] \subseteq [2, 2, 1, 1] \cdot [2, 2] && \text{by } O_2(\text{d}),\\ &[3, 3] \subseteq [2, 1, 2, 1] \cdot [2, 2] && \text{by } O_2(\text{d}). \end{aligned}$$

Finally

$$[3, 2] = [3, 1, 2] \subseteq [6] \cdot [2, 2] \subseteq B_\tau(3+2)$$

by O_2(a). This exhausts all the nontrivial conjugacy classes in S_6 and therefore $\|S_6\|_\tau \le 5$ as needed.

We now assume that $n \ge 7$ and that $\Delta(S_m) = m-1$ for all $2 \le m < n$. Choose an odd permutation $\tau \in S_n$ without fixed points. If τ is an n-cycle then $\|S_n\|_\tau \le n-1$ by Proposition 4.15. So we assume that τ is a product of at least two cycles each of length $k \ge 2$. If one of these cycles has odd length $k \ge 3$ then $n-k \ge 2$ (or else τ has a fixed point) and Proposition 4.13, together with the induction hypothesis, shows that

$$\|S_n\|_\tau \le \Delta(S_{n-k}) + k = n-k-1+k = n-1$$

as needed. If τ contains no cycles of odd length then it is a product of cycles of even length. Since τ is odd, the number of these cycles must be odd, and since τ is not a cycle, it is a product of at least three cycles of even length. Let $p \ge q$ be the lengths of the shortest two cycles in τ. Then $q \ge 2$ and $n-(p+q) \ge p$ because τ contains a third cycle of length at least p. Appealing to Proposition 4.14 and the induction hypothesis, we deduce that

$$\|S_n\|_\tau \le \Delta(S_{n-p-q}) + p + q = n-1.$$

The induction step is complete. □

References

[Babai and Seress 1992] L. Babai and A. Seress, "On the diameter of permutation groups", *European J. Combin.* **13**:4 (1992), 231–243. MR Zbl

[Babai et al. 1990] L. Babai, G. Hetyei, W. M. Kantor, A. Lubotzky, and A. Seress, "On the diameter of finite groups", pp. 857–865 in *31st Annual Symposium on Foundations of Computer Science, Vol. II* (St. Louis, MO, 1990), IEEE Comput. Soc. Press, Los Alamitos, CA, 1990. MR

[Bardakov et al. 2012] V. Bardakov, V. Tolstykh, and V. Vershinin, "Generating groups by conjugation-invariant sets", *J. Algebra Appl.* **11**:4 (2012), art. id. 1250071. MR Zbl

[Burago et al. 2008] D. Burago, S. Ivanov, and L. Polterovich, "Conjugation-invariant norms on groups of geometric origin", pp. 221–250 in *Groups of diffeomorphisms*, edited by R. Penner et al., Adv. Stud. Pure Math. **52**, Math. Soc. Japan, Tokyo, 2008. MR Zbl

[Hall 1959] M. Hall, Jr., *The theory of groups*, The Macmillan Co., New York, 1959. MR Zbl

[Helfgott and Seress 2014] H. A. Helfgott and A. Seress, "On the diameter of permutation groups", *Ann. of Math.* (2) **179**:2 (2014), 611–658. MR Zbl

[Kędra et al. 2018] J. Kędra, A. Libman, and B. Martin, "Strong and uniform boundedness of groups", preprint, 2018. arXiv

[Klopsch and Lev 2003] B. Klopsch and V. F. Lev, "How long does it take to generate a group?", *J. Algebra* **261**:1 (2003), 145–171. MR Zbl

[Preparata and Vuillemin 1981] F. P. Preparata and J. Vuillemin, "The cube-connected cycles: a versatile network for parallel computation", *Comm. ACM* **24**:5 (1981), 300–309. MR

[Rotman 1973] J. J. Rotman, *The theory of groups: an introduction*, 2nd ed., Allyn and Bacon, Boston, MA, 1973. MR Zbl

[Tarry 2020] C. Tarry, "Strong and uniform boundedness of groups", undergraduate project, 2020.

Received: 2020-03-04 Revised: 2020-05-10 Accepted: 2020-06-25

a.libman@abdn.ac.uk *Institute of Mathematics, University of Aberdeen, King's College, Aberdeen, United Kingdom*

charlotte0687@hotmail.co.uk *Institute of Mathematics, University of Aberdeen, King's College, Aberdeen, United Kingdom*

mathematical sciences publishers msp

involve

msp.org/involve

INVOLVE YOUR STUDENTS IN RESEARCH

Involve showcases and encourages high-quality mathematical research involving students from all academic levels. The editorial board consists of mathematical scientists committed to nurturing student participation in research. Bridging the gap between the extremes of purely undergraduate research journals and mainstream research journals, *Involve* provides a venue to mathematicians wishing to encourage the creative involvement of students.

See inside back cover or msp.org/involve for submission instructions. The subscription price for 2020 is US $205/year for the electronic version, and $275/year (+$35, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840, is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

involve

2020 vol. 13 no. 4

1944-4176(2020)13:4;1-Q